Claim 5 is objected to because of informalities. Claim 5 has accordingly been amended.

Claims 1-22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes et al., Handbook of Applied Crytography, (hereinafter "Menezes"). The rejection is respectfully traversed.

With regard to independent claims 1 and 12, it is asserted by the Examiner that Menezes teaches the features of claim 1, except that a value R_a is used instead of a "count value" as claimed. It is further asserted by the Examiner that Menezes teaches interchangeability in authentication protocols. We respectfully disagree.

A close review of the teaching of Menezes reveals that section 10.3.1 teaches that various time variant parameters may be used in identification protocols, and that such parameters are loosely defined as specific properties associated therewith depend on actually usage and protocols. Menezes further provides examples of various types of time variant parameters including, for example, random numbers, sequence numbers, and time stamps, and the advantages and disadvantages associated with each. It is nowhere suggested in Menezes that each specific type of time variant parameter is "interchangeable". It is further respectfully submitted that the applied reference, being theoretical in nature, at best, may suggest that one of advanced skill in the art *could* eventually be led to the invention, however, this does not amount to establish a *prima facie* case of

obviousness. Moreover, a close review of the description on page 402 reveals a three-pass challenge response mechanism based on a MAC algorithm. It should be noted that a MAC algorithm amounts to a keyed hash algorithm and does not amount to a teaching or suggestion of the key cryptographic function as recited, for example, in claim 1. Menezes further fails to teach or suggest incrementing a count value in response to receiving a first challenge, generating a first challenge response by performing a keyed cryptographic function (KCF) on the first challenge in the count value using a first key, transferring the count value as a second challenge and the first challenge response to the first party, receiving a second challenge response from the first party being a result of performing the KCF on the second challenge using the first key, and verifying the first party based on the second challenge and the second challenge response. It should be noted that the three-pass challenge response mechanism shown on page 402 is designed to provide mutual identification. Accordingly, in the third message additional field A is provided for identification and does not amount to a teaching of a count value.

Claim 1 can be further distinguished from Menezes in that the first party is verified after receiving a second challenge response being a result of performing a KCF on a second challenge only using a first key. The inclusion of additional field A strongly suggests that the mutual identification three pass challenge response mechanism shown on page 402 of Menezes represents an approach to an entirely

different problem and is based on a keyed hash algorithm rather than the KCF of the claimed invention. Accordingly, it is respectfully submitted that Menezes fails to teach or suggest all of the elements of the claimed invention as required. It is respectfully requested therefore that the rejection of independent claims 1 and 12 be reconsidered and withdrawn.

With regard to claims 2-11 and 13-22, it is respectfully submitted that in depending from claims 1 and 12, believed allowable for at least the reasons set forth hereinabove, claims 2-11 and 13-22 are also allowable. In addition, it is respectfully submitted that independent grounds may exist for the allowability of claims 2-11 and 13-22.

INDEPENDENT GROUNDS FOR ALLOWABILITY

It is respectfully submitted that, as previously submitted, independent grounds may exist for the allowability of claims 2-11 and 13-22. Such grounds include at least the following.

With regard to claim 3, it is asserted by the Examiner that Menezes teaches including identification information "B" in a corresponding response, for example, at page 402. It is respectfully submitted that for at least the reasons as set forth hereinabove with regard to claim 1, e.g. that Menezes fail to teach or suggest, for example, incrementing a count value that Menezes further necessarily fails to teach or suggest generating the first challenge response by performing a KCF on

the first challenge, the count value, and identifier for the second party using the first key. It is submitted therefore that claim 3 is independently allowable.

With regard to claim 4, it is asserted by the Examiner that the SKID3 protocol, which teaches not an encryption function but a keyed hash algorithm, or MAC algorithm (page 402 section 10.17(ii) line 7), amounts to a teaching or suggestion that a second key is established based on a first and second challenge. We disagree and submit that Menezes fails to teach or suggest establishing a second key. Accordingly, it is respectfully submitted that claim 4 is independently allowable.

With regard to claim 7, as best understood, the Examiner is using claim 7 in combination with Menezes in a circular manner to arrive at claim 7. it is respectfully submitted that a teaching that information is included regarding a form of a challenge in an identifier does not amount to a teaching of a type of authentication protocol. Moreover, it should be noted that a challenge is simply one aspect of any given protocol and the form of a challenge does not necessarily dictate the type of protocol. It is further respectfully submitted that using claim 7 and Menezes in this manner amounts to improper hindsight reasoning using the teachings of Applicants specification.

With regard to claim 8, it is respectfully submitted that, for at least the reasons set forth hereinabove, e.g. Menezes fails to further suggest, for example,

performing a KCF on a first challenge, a count value and type data, claim 8 is independently allowable.

With regard to claim 10, it is asserted that key K of Menezes amounts to a teaching of, for example, a second shared key. It is respectfully submitted that key K of Menezes cannot serve as both the first key as also alleged in the rejection of claim 1 and the second key as alleged here. It is respectfully submitted therefore that Menezes fails to teach, for example, a second key and in so submitting, Applicant is not making any admission as to whether or not Menezes teaches the first key. Accordingly, it is respectfully submitted that claim 10 is independently allowable.

With regard to claim 11, it is respectfully submitted that, for at least the reasons as set forth hereinabove, e.g. that Menezes fails to teach or suggest a count value, and that Menezes fails to teach using a bit counter of greater than 64 bits, which is initialized using a random number claim 11 can be distinguished over Menezes. The Examiner asserts that the choice of 64 bit or greater counter value would have been an obvious design choice. Applicant respectfully disagrees. It should be understood that using a bit counter of greater than 64 bits allows certain advantages to be realized in, for example, accordance with a preferred embodiment, e.g. managing keys of a certain size. Further, it is merely asserted that initializing a counter with a random number is standard practice. Applicant knows however, of no art, which teaches or suggest using initialization with a

random number in combination with other claimed elements to arrive at the claimed invention. It is therefore requested that art be provided which teaches or suggest this element. Alternatively, it is respectfully submitted that Menezes fails to teach or suggest all of the limitations of claim 11 and that claim 11 is therefore independently allowable.

With regard to dependent claims 13-22, it is respectfully submitted that for at least the reasons as set forth with regard to corresponding ones of claims 2-11 that, for example, claims 14, 15, 18, 19, 21, and 22 are also independently allowable.

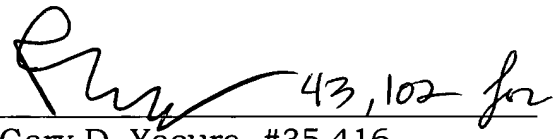
CONCLUSION

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Robert L. Scott (Reg. No. 43,102) at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 12-2325 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By  43,102 for
Gary D. Yacura, #35,416

GDY/RLS/tmd
2925-0161P

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000